NVSS

IRD1, Nintendo

APR, 2014

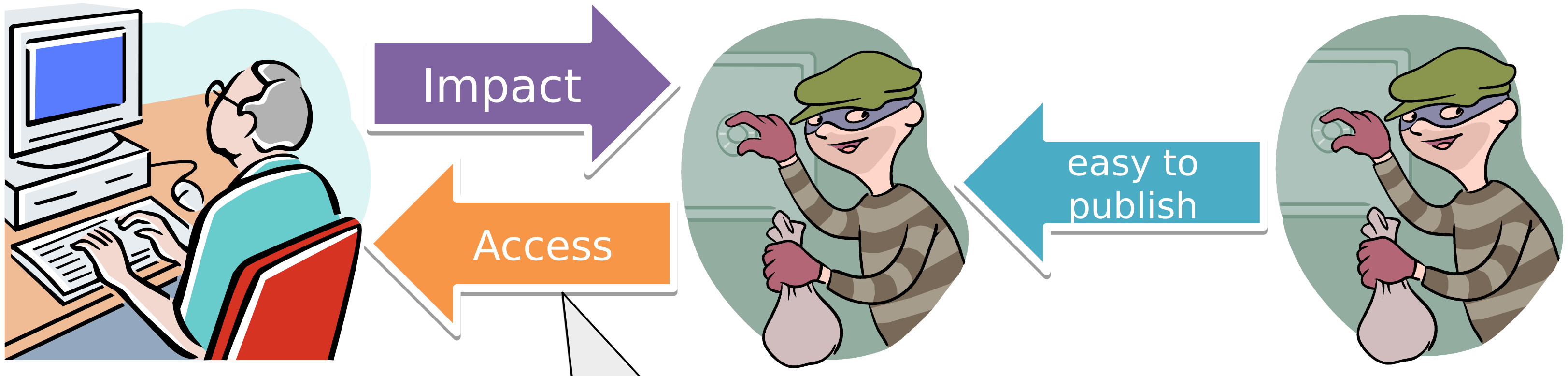
CVSS

Good User Model

Security Fault

Use Exploit

Create Exploit



Impact

Access

easy to publish

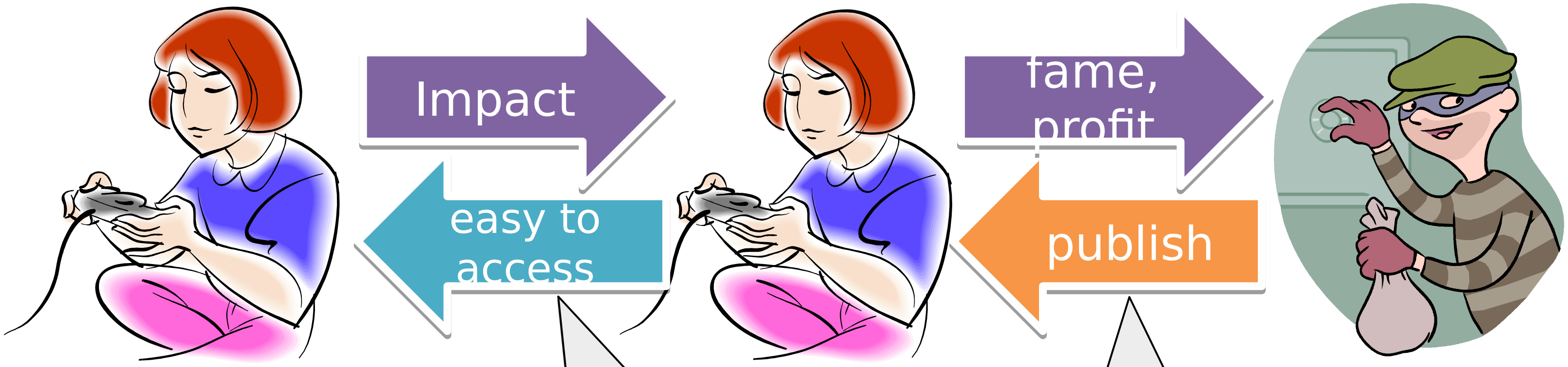
1. Confidentiality Impact
2. Integrity Impact
3. Availability Impact

1. Access Vector
2. Access Complexity
3. Authentication

Lacking case in CVSS

Piracy Model

Security Fault Use Exploit Create Exploit



Impact

easy to access

fame, profit

publish

1. Confidentiality Impact
2. Integrity Impact
3. Availability Impact

1. ~~Access Vector~~
2. Access Complexity
3. ~~Authentication~~
4. Using Complexity

1. Productivity
2. Availability
3. Legality

New Metrics

- Using Complexity Risk
  - mod chip (Low) / other (High)
- Productivity Risk
  - Hardware (Low) / Software (High)
- Availability Risk
  - physical (Low) / Internet (High)
- Legality Risk
  - illegality (Low) / gray (Middle) / legally (High)

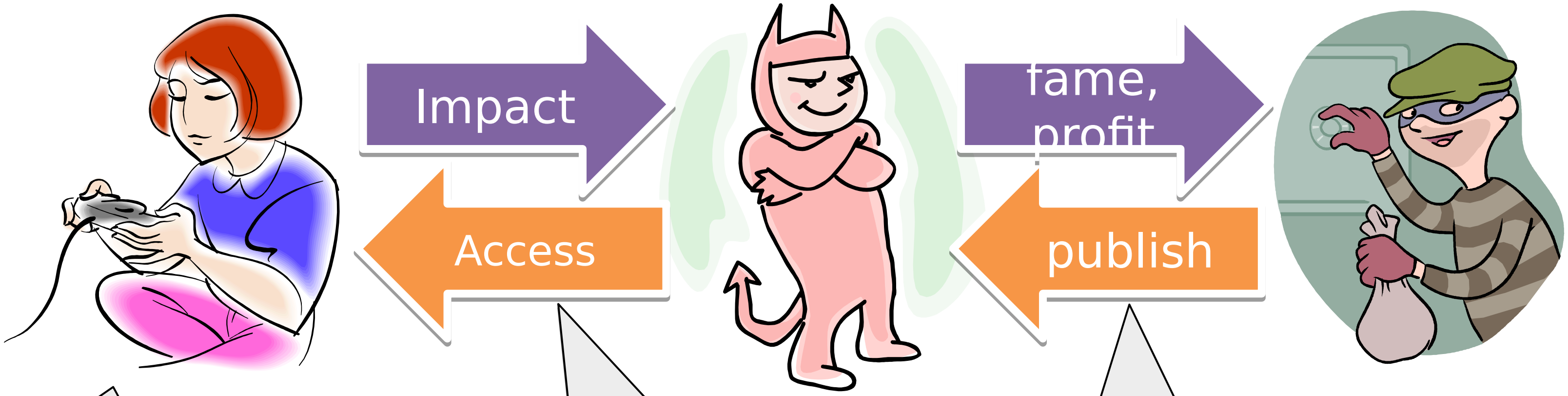
NVSS

General Model

Security Fault

Use Exploit

Create Exploit



Impact

Access

fame, profit

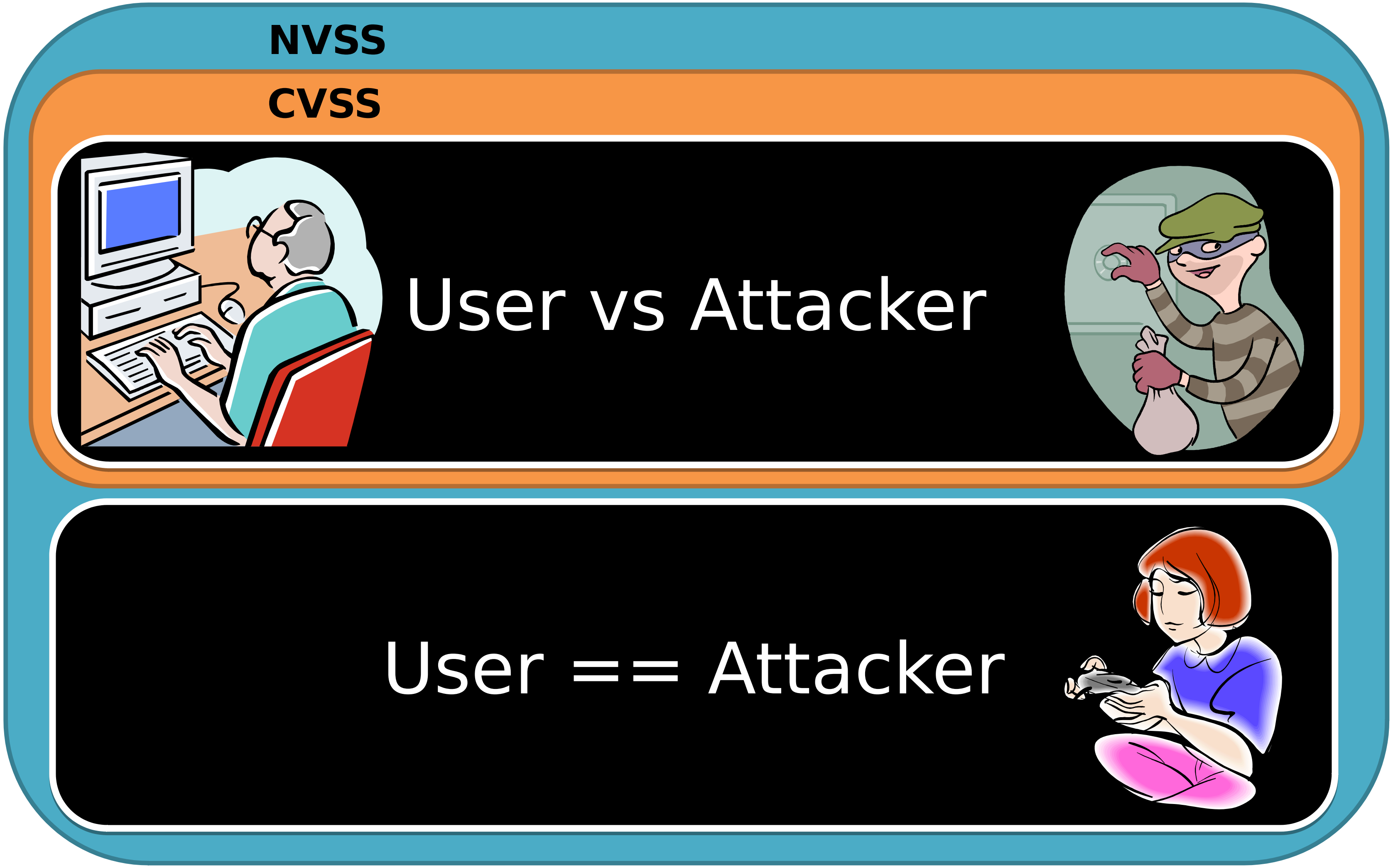
publish

1. Confidentiality Impact
2. Integrity Impact
3. Availability Impact

1. Access Vector
2. Access Complexity
3. Authentication
4. Using Complexity

1. Productivity
2. Availability
3. Legality

CVSS → NVSS



NVSS

CVSS

User vs Attacker

User == Attacker

use case 1
ARM9 injection from website

	N/A case	
Productivity	Attacker == Hacker	
Availability	Attacker == Hacker	
Legality	Attacker == Hacker	
Access Vector	User == Attacker	Remote
Access Complexity		Under 4.5 firmware
Authentication	User == Attacker	Needless
Using Complexity		Internet brouser
Confidentiality Impact	-	All

Base Metric s

9.3

Temp Metric s

8.4

use case 2
parental tool

	N/A case	
Productivity	Attacker == Hacker	Software
Availability	Attacker == Hacker	Download
Legality	Attacker == Hacker	Legality
Access Vector	User == Attacker	Local
Access Complexity		Under 5.5 firmware
Authentication	User == Attacker	Needless
Using Complexity		PC software
Confidentiality Impact	-	Nothing

Base Metrics

4.3

Temp Metrics

3.9

use case 3
Gateway3DS

	N/A case	
Productivity	Attacker == Hacker	Existing hardware
Availability	Attacker == Hacker	Physical
Legality	Attacker == Hacker	gray
Access Vector	User == Attacker	N/A
Access Complexity		Under 4.5 firmware
Authentication	User == Attacker	N/A
Using Complexity		Cartridge
Confidentiality Impact	-	All

Base Metrics

6.9

Temp Metrics

6.2

use case 4
MSET vuln

	N/A case	
Productivity	Attacker == Hacker	Hardware
Availability	Attacker == Hacker	Physical
Legality	Attacker == Hacker	Illegal
Access Vector	User == Attacker	N/A
Access Complexity		Under 6.0 firmware
Authentication	User == Attacker	N/A
Using Complexity		Cartridge
Confidentiality Impact	-	Part

Base Metrics

3.9

Temp Metrics

3.4

use case 5
sandbox vuln

	N/A case	
Productivity	Attacker == Hacker	Hardware
Availability	Attacker == Hacker	Physical
Legality	Attacker == Hacker	
Access Vector	User == Attacker	N/A
Access Complexity		Under 6.0 firmware
Authentication	User == Attacker	N/A
Using Complexity		Need entry point
Confidentiality Impact	-	Part

Base Metrics

6.8

Temp Metrics

2.5

use case 6
process9 vuln

	N/A case	
Productivity	Attacker == Hacker	Hardware
Availability	Attacker == Hacker	Physical
Legality	Attacker == Hacker	
Access Vector	User == Attacker	N/A
Access Complexity		Under 6.0 firmware
Authentication	User == Attacker	N/A
Using Complexity		Need entry point
Confidentiality Impact	-	All

Base Metrics

9.3

Temp Metrics

3.4